Performance Work Statement
Defense Manpower Data Center (DMDC) Enterprise
Information Technology Services (EITS) I I
DMDC Enterprise Development Operations (DEVOPS)

Enterprise Development Operations (DEVOPS)
EITS II Task Order
Order ID No: 47QFMA18K0030-0018

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) requires information technology services to support the implementation, configuration and maintenance of an Enterprise Development Operations (DEVOPS) infrastructure and supporting processes for the DMDC Enterprise Development Environments to be located in DMDC's enterprise software hosting environment.

2.0 BACKGROUND

Development Operations (DEVOPS), henceforth referred to as DevSecOps, emphasizing the importance of security within the domain, is the collaboration, integration and communication of both software developers and other IT Professionals focused on the automation of software delivery and infrastructure changes to deliver business capabilities in a manner that reduces cost and increases business value. The adoption of this methodology is supported and enforced through the implementation of automation tools that will increase standardization and dependability when integrated as a unified system.

With the higher adoption of the Agile Software Development methodology and the strain of reduced budgets within the Department of Defense, DMDC needs to ensure timely delivery of defect free code to its production environment while reducing the dependency on touch labor to realize this increased productivity level. This is compounded with the need to ensure security standards are enforced and auditability is maintained without sacrificing that agility. The new DMDC DevSecOps environment will be an integrated ecosystem comprised of continuous deployment; continuous integration and continuous quality assurance in order to affect application release and infrastructure build automation accomplishing a complete end-to-end continuous delivery mechanism.

3.0 SCOPE

The Contractor shall provide the personnel and management necessary to enable DMDC to implement and maintain the processes and environment to produce an optimized Enterprise DevSecOps Environment utilizing Government Furnished Equipment and Software. This will also require constant coordination with the Service Delivery (SD) and Technical Services (TS) Directorates in order to facilitate workload changes into the toolset pipeline.

4.0 REQUIREMENTS. *The Contractor shall support:*

4.1 CONTINUOUS INTEGRATION INFRASTRUCTURE

4.1.1 Sustain and enhance the Enterprise Continuous Integration Infrastructure and its related process workflows to support DMDC Continuous Integration. All requirements, plans, process workflows and required system specifications will be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of, and be approved by, the DMDC

Architecture Review Board before implementation by the contractor will be authorized. This shall include the sustainment and enhancement of the:

4.1.1.1 Scalable Continuous Integration orchestration infrastructure in the DMDC Enterprise Development and Testing Environments utilizing the Government provided tools. Enhancements shall include configuration and maintenance of Architecture Review Board (ARB) approved technologies and architectures for container orchestration.

4.1.1.2 Software configuration management system in the DMDC Enterprise Development and Testing Environments.

4.1.1.3 Integrated source code repository, which is capable of providing version control for multiple coding languages and platforms (Java, .Net, JavaScript, Ruby, Python and others as identified), utilized for the consolidation of all DMDC source code repositories.

4.1.1.4 Integrated build automation tool and repository, which is capable of providing on-demand and triggered automation tasking for continuous integration activities to be utilized as the centralized DMDC build automation repository for DMDC developed applications.

4.1.1.5 Job automation templates, utilizing the Government provided toolsets that enable on-demand, unattended application builds and deployments of DMDC developed applications through all build, test and production environments to their authorized containers segments as designated in the Configuration Management Repository.

4.1.1.6 Job automation templates, utilizing the Government provided Jenkins Template Toolset that will enable on-demand, unattended database schema builds and deployments through all build, test and production environments to their authorized multi-tenet database segments as designated in the Configuration Management Repository.

4.1.1.7 Process workflows and orchestration engine that enable the on-demand automation of Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) compliant creation and configuration of virtual workstations and servers, network instantiation, application build, test and release, as well as registering all required Configuration Item attributes into the Central Configuration Repository.

4.1.1.8 Process workflows and orchestration engine automation, utilizing the Government provided Information Technology Service Management (ITSM) workflow management toolset, that will automate Continuous Integration tasks (build, test and deploy) based on request, issue tracking and resolution events in the centralized Change Management Database (CMDB).

4.1.1.9 Automated verification and update of all configuration management attributes for application and database deployments and changes in the Government provided central configuration management repository.

4.1.1.10 Automated verification and update of all dependency attributes (software libraries) for application and database deployments and changes in the Government provided central configuration management repository.

4.1.1.11 Process and procedures that enable DMDC software developers to commit code changes to the repository daily for insertion into the Continuous Integration workflow.

4.1.1.12 Processes for automating the download of DMDC approved commercial software code libraries from only DMDC approved code sources upon request submitted through the Change Request

system.

4.1.1.13 Automated procedures, workflows, form wireframes scripting and dashboards to be implemented through the ITSM workflow management toolset to allow for visibility and auditing of each step in the Continuous Integration process flow.

4.1.1.14 Architecture, analysis, design, and maintenance documentation for executing Continuous Integration processes and procedures, and update of the associated artifacts within 10 business days of change.

4.2 CONTINUOUS DEPLOYMENT TESTING INFRASTRUCTURE

4.2.1 Sustain and enhance the Enterprise Continuous Deployment Testing Infrastructure and its related process workflows to support DMDC Continuous Deployment Testing. All recommendations, plans, process workflows and required system specifications will be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review Board. This shall include:

4.2.1.1 Sustainment and enhancement of the process workflows to enable the automation of the Government provided Quality Assurance tools Redwood HQ, SOAPUI, Selenium and Junit throughout the Software Development Lifecycle (SDLC) process to allow developers access in any phase of deployment.

4.2.1.2 Sustainment and enhancement of the core functional testing capabilities in the automated Continuous Integration process by utilizing pre-defined Quality Assurance Test Cases to be provided by the Government Quality Assurance (QA) staff.

4.2.1.3 Sustainment and enhancement of the centralized dashboard that analyzes data captured in the DMDC Enterprise Continuous Deployment Testing infrastructure that will register bugs or issues in a central issue tracking repository, email alerts upon discovery of an issue or failure, allow for creation of customizable reports and provide application specific details.

4.2.1.4 Architecture, analysis, design, and maintenance documentation for executing continuous integration test cases, and update the associated artifacts within 10 business days of change.

4.3 APPLICATION SECURITY TESTING INFRASTRUCTURE

4.3.1 Sustainment and enhancement of the Enterprise Continuous Application Security Testing Infrastructure and its related process workflows as a recommendation for implementation in DMDC's enterprise software hosting environment to support DMDC Continuous Application Security Testing. All recommendations, plans, process workflows and required system specifications shall be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review. This shall include sustainment and enhancement of the:

4.3.1.1 Government provided security testing tools, Sonatype (library compliance), Fortify (static code analyzer) and WebInspect (dynamic code analyzer) in order to provide automated, and on-demand through ITSM workflow automation toolset, application security testing to meet the requirements under the Enclave and Developers Security Technical Implementation Guide (STIG).

4.3.1.2 Centralized dashboard that analyzes data captured in the DMDC Enterprise Application Security Testing infrastructure that will email alerts upon discovery of an issue or failure, allow for creation of customizable reports and provide application specific security details.

4.3.1.3 Provide architecture, analysis, design, and maintenance documentation for executing continuous integration test cases, and update the associated artifacts within 10 days of change.

4.4 PERFORMANCE TESTING INFRASTRUCTURE

4.4.1 Sustain and enhance the Enterprise Performance Testing Infrastructure and its related process workflows to support DMDC Application Performance Testing. All recommendations, plans, process workflows and required system specifications will be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review Board. This shall include sustainment and enhancement of the:

4.4.1.1 Performance testing harness that will provide DMDC application load and stress functionality in an on-demand fashion using the Government provided testing software.

4.4.1.2 Automated performance testing process workflows that will evaluate the responsiveness, speed, scalability and stability characteristics of DMDC applications. Leverage applicable test case scenarios currently supported by the development and QA teams as applicable.

4.4.1.3 Automated load testing process workflows that will constantly and steadily increase the load on the identified system until the time it reaches the threshold limit. The goals of load testing are to expose the defects in application related to buffer overflow, memory leaks and mismanagement of memory. Another target of load testing is to determine the upper limit of all the components of application like database, hardware and network etc.

4.4.1.4 Automated stress testing process workflows that will evaluate the applications behavior beyond normal or peak load conditions. Test the functionality of the application under high loads.

4.4.1.5 Centralized dashboard that analyzes data captured in the DMDC Enterprise Performance Testing infrastructure that will email alerts upon discovery of an issue or failure, allow for creation of customizable reports and provide application specific performance details.

4.4.1.6 Architecture, analysis, design, and maintenance documentation for executing Application Performance Testing, and update the associated artifacts within 10 business days of change.

4.5 PROVIDE APPLICATION MONITORING SUPPORT

4.5.1 Working with IT Operations (ITOps), support shall be provided to ensure monitoring of the DevSecOps infrastructure can be adequately performed. This will require regular interaction with ITOps and the tools used to perform monitoring tasks.

4.5.2 DevSecOps monitoring shall include (but may not be limited to) monitoring of container infrastructure, container network infrastructure, as well as the build and deployment systems.

4.5.3 Any monitoring components installed within the DevSecOps infrastructure shall integrate with enterprise monitoring implementations. Sustainment of this infrastructure must be performed during the performance period.

4.6 APPLICATION RESILIENCE TESTING

4.6.1 Sustain and enhance the Enterprise Application Resiliency Testing process workflows as a recommendation for implementation in DMDC's enterprise software hosting environment to support DMDC Application Resilience Testing. All recommendations, plans, process workflows

and required system specifications shall be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review Board before implementation by the contractor will be authorized. Resiliency Testing is defined as the process of subjecting an application or IT system to unforeseen events and documentation of the results of system behavior induced by the event. These events may include a power outage, running out of disk space, network outages, etc. The goal of this testing is to ensure that these unforeseen events do not result in the loss of any data.

4.6.2 Architecture, analysis, design, execution and maintenance documentation for executing the DMDC Resiliency Test Plan, and update the associated artifacts within 10 business days of change.

4.7 (OPTIONAL CLIN)(T&M) DEVSECOPS IMPLEMENTATION SUPPORT FOR TRANSITION TO A NEW PLATFORM/ARCHITECTURE (CLOUD, AWS, MILCLOUD, ETC)

4.7.1 Provide DMDC with best practices, industry knowledge and expertise, and technical support, during and after DevSecOps implementation in DMDC's enterprise software hosting environment. Implementation will be completed within 90 days

4.7.2 Update DevSecOps implementation plan within 5 business days of any changes; develop and monitor implementation schedule and facilitate implementation status meetings.

4.7.3 Perform research to validate that reported defects are defects. Determine root cause of software problems and recommend remediation. Triage defects reported by the customers and assigned a 'priority level'.

4.7.4 Assist in ad hoc reporting and serve as point of contact between product development group and customers.

4.7.5 Provide a monthly report on implementation status reporting and schedule.

5.0 REPORTS AND MEETINGS

Unless specified elsewhere within this PWS, all reports and deliverables shall be submitted in Microsoft Office products to include Microsoft Project and shall be accessible via web. All diagrams shall be delivered in a readable format (PDF or standard formats and hard copy (including oversized diagrams).

5.1 PROGRAM MANAGEMENT PLAN (PMP)

Provide a draft Program Management Plan (PMP) to the COR within 10 business days of award that describes the overall approach to managing the DEVOPS requirements. This PMP shall include the contractors overall management approach, quality control plan, operating procedures, staffing approach, milestones, tasks, subtasks and the overall Work Breakdown Structure (WBS). The PMP shall identify and assign tasks, major milestones, dates and dependencies, and indications of critical path. Tasks from the final Government-approved PMP shall be selected as milestones against which Contractors' progress is monitored. The PMP shall include milestones and measurable indicators that can be used to evaluate satisfactory progress toward delivering services. The Contractor shall include in the PMP: the status, statistics; risk management review; critical path and other milestone progress checks and updates; as well as technical content review. The program plan shall be finalized 45 business days after TO award via deliverables acceptance criteria under PWS Section 5.0 – "Deliverables." The PMP may be updated, after discussions and mutual agreements, as a result of changes in priorities or the receipt and acceptance of new deliverables.

5.2 KICK-OFF MEETING

This meeting provides an introduction between the Contractor and Government personnel who will be involved with the TO and will aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. This meeting is not a substitute for the contractor to fully understand the work requirements. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Kick Off Meeting to the DMDC COR, and GSA COR within 3 business days.

5.3 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

Prior to the delivery of the monthly SMR, the contractor shall also hold monthly pre-SMR meetings with designated Government representatives for each awarded task order. The purpose of the pre-SMR meeting shall be to present the same documentation that will be presented at the official SMR while also reviewing each task order's specific task order data (listed above). Each contractor task order manager shall coordinate the pre-meeting, distribute the pre-meeting materials and facilitate any changes to the task order's data through the DMDC COR and contractor Program Manager.

5.4 Problem Notification Reports

The Contractor shall follow the requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

6.0 Deliverables

All deliverables and work products shall be submitted to the COR in electronic format for acceptance and approval. The acceptance of deliverables and satisfactory work performance shall be based on the timeliness, accuracy and standards as specified in the requirements of the PWS.

Deliverable	PWS	Delivery Date
Enterprise Continuous Integration System Engineering	4.1.1	Continuous
Enterprise Continuous Deployment Testing System Engineering	4.2.1	Continuous
Enterprise Application Security Testing System Engineering	4.3.1	Continuous
Enterprise Performance Testing System Engineering	4.4.1	Continuous
Enterprise Application Resiliency Testing System Engineering	4.6.1	Continuous
Implementation Support	4.7	Continuous
Update Implementation Plan	4.7.2	Within 5 business days of change
Implementation Status Monthly Report	4.7.5	Monthly

Program Management Plan	5.1	Draft submitted within 10 business days of order award; Final submitted within ten days after receipt of Government comments. Updates as needed and no less frequently than 30 days after exercise of an Option
Post Award Conference	5.2	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
SMR Documentation	5.3	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
Problem Notification Reports	5.4	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ

7.0 QUALITY SURVEILLANCE

The Government may follow the Appendix P - Quality Assurance Surveillance Plan) to EITS II IDIQ Base Contract

8.0 Performance Objective and Thresholds:

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.
Key Personnel: Provide qualified personnel in a timely manner.	New or replacement personnel in place within fourteen (14) calendar days of negotiated date.

8.1 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.

- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.
- Timeliness – Deliverables shall be submitted on or before the due date specified

9.0 Contract Administration.

This Task Order shall follow all of the requirements identified in the EITS II IDIQ.

9.1 Contract Type: The contract type for this Task Order will be firm fixed price

9.2 Period of Performance: The period of performance for this Task Order shall be 12 months from date of award with two one-year options.

9.3 PLACE OF PERFORMANCE / HOURS OF OPERATION: At least 50% of the work under this task will be performed on site at DMDC facilities in Seaside, CA. The remaining percentage of work may be performed at a contractor provided facility. Any work performed at other locations must be identified in the formal submission and approved by the Government. Occasional travel may also be required, as noted in PWS Section - Travel.

The contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m. ET (8 a.m. to 5 p.m. PT for contractors located on the West Coast), Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

9.4 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

9.5 Points of Contact:
DMDC COR will be assigned Post Award

GSA Contracting Officer (CO)
Mr. David Long
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: David.Long@gsa.gov
Tel: 215-446-4597

GSA Contract Specialist (CS)
Mr. Raj Singh
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West

Philadelphia, PA 19106
E-mail: rajdeep.singh@gsa.gov
Tel: 215-446-2868

GSA Contracting Officer's Representative (COR)
Mr. Scott Ostrow
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Scott.ostrow@gsa.gov
Tel: 215-446-4497

9.6 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI): The Contractor shall follow the requirements identified in the PWS Sections 10.8 thru 10.9 of the EITS II Base IDIQ

9.7 Travel: The cost reimbursable not-to-exceed travel limit is estimated at $5,000.00 per year. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR. All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

9.8 Security: The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

In addition, certain contractor personnel under this task order shall hold fully-adjudicated and active Secret security clearances, as directed by the Government. Contractor personnel shall possess these security clearances at Task Order award.

10.0 INSPECTION, ACCEPTANCE AND PAYMENT

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

11.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf